REMARKS

In the Office Action mailed February 11, 2004, Examiner rejected the claims as anticipated by United States Patent No. 6,532,542 to Thomlinson et al.

The present invention is for authenticating a user locally, that is, at a computer which is remote from a server to which the remote computer is networked, and then using the local data to generate an encryption key for transmitting data from the remote computer to the server. In the present invention, the encrypted data file is a name for a string of data. The string of data is encrypted with the password provided by the user. Once decrypted, this string of data becomes a component to form the key of the user. The string of data may contain user biometrics such as a fingerprint biometric template. This string of data becomes the basis for encrypting data to be transmitted to the server, without the password or biometric template data being sent to the server. Hence security is enhanced if this core secret data is never in the server.

Thomlinson et al. disclose only the use of a central server for storing or for directing the storing in storage devices of core data secrets such as cryptographic keys. See for example references on Thomlinson at column 1 lines 11-12 ("central services"), and line 61 ("central protected storage services:), and in column 2 lines 6, 11 (reference to "calling application programs"), and in column 6 lines 19-22 ("the protected storage system allows application programs to securely store data items that must be kept private...such data items might include cryptographic keys...the storage system is designed to hold small items of core secret data in a central and common storage location"), and in column 7, line 18, reference to storage server 102, and in column 13 lines 30-32 "different application programs can utilize a single provided server to store core data secrets in a central storage area." Calling applications and the protected storage system may be in the server, but in different address spaces, communication therebetween using remote procedure calls (column 7 lines 20-24). Authentication providers are called by the storage server to identify and/or authenticate current computer users (column 6 lines 49-51).

As Thomlinson states in column 7, line 6: "A smart card authentication provider might similarly be provided to authenticate users". This specifically precludes the use of the local or remote authentication system of the present invention in a system using the Thomlinson invention. Consequently, Thomlinson, in solely teaching the use of a server doing or directing the authentication (i.e. dealing with the core date secrets), teaches away from the remote authentication according to the present invention wherein the server has no contact with the core date secrets used for authentication..

As Thomlinson states in column 7, line 8: "In either case, the smart card could utilize public-key cryptographic techniques". This statement implies that the data items on the smart card are then transferred to the storage server via PKI methods.

Finally, referring now to the process taught by Thomlinson beginning in column 11, line 1: "To generate the user key, the user-supplied password is appended to a random number referred to as salt and hashed in a step using an SHA-1 hashing function. This results in a number that is used as the user key", applicant advises that this will not work and results in the problem that the present invention overcomes. The problem is that this procedure of Thomlinson is not possible to reverse in order to recover the data encrypted with the derived key. If it is possible to reverse, then the random number is not random but specified and if the number is specified, where is it kept? This is specifically the problem that the current invention circumvents. In the present invention the user supplied credentials are only used locally and are not used at either the application server or the storage server as is done by Thomlinson and known in the prior art. In the present invention the password is not transmitted to the server as is done by Thomlinson, nor are the components of the user key transmitted to the central storage system.

The independent claims have been amended to clarify this distinction, and new claim 42 added which also contains the patentable distinction that the computer components and functions including the decrypt engine, the use of the user supplied password to allow decryption of an encrypted core secret data string, such as may contain a unique user biometric template, so as to form an encryption key which is then used to encrypt data for transmission to a server, all occurs only in a local, that is, remote computer networked to the server computer, and without

any transmission to the server of the password, or the encrypted core secret data, or decryption key formed therefrom.

Applicant consequently submits that the claims as currently amended, and new claim 42, patentably distinguish over Thomlinson. In response to the 35 U.S.C. 112 objection, applicant submits that the claims as amended are definite in that it is clear that the encrypted data file containing the core secret data is decrypted locally and then used to form an encryption key for local encryption of data to be transmitted from the local computer.

REQUEST FOR EXTENSION OF TIME UNDER 37 CFR, SECTION 1.136

Applicant hereby requests a 1 month extension of time to respond to the Office Action to and through June 11, 2004.

Examiner is respectfully requested to now pass this application to allowance.

Respectfully submitted,
Lynn D. Spraggs

By: 
Antony C. Edwards
Registration No. 40,288

May 18, 2004
ACE/mh/ds

800 – 1708 Dolphin Avenue
Kelowna, British Columbia, Canada
V1Y 9S4

Telephone: (250) 861-5332
Facsimile: (250) 861-8772

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Diana Sposato
Name of Person Signing Certification

Signature

May 27/04
Date